IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE-BCM

DECLARATION OF STEVEN COLQUITT IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

I, Steven Colquitt, hereby declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, as follows:

I. INTRODUCTION

1. I am currently the Head of Engineering at SS&C Blue Prism, an enterprise AI and automation company. Previously, I served in various software engineering positions at SolarWinds (the "Company"), including as a Director of Engineering from 2015 to 2023, and a Senior Director of Engineering from 2023 to 2025. I make this declaration in support of SolarWinds and Tim Brown's motion for summary judgment. The facts set forth herein are based on my personal knowledge and my review of SolarWinds records. If called upon to do so, I can and will competently testify to these facts.

2. I understand that the Securities and Exchange Commission (SEC) relies on an email that I wrote during my tenure at the Company to argue that certain representations in SolarWinds' online Security Statement were false or misleading. Specifically, I understand that the SEC relies on an email I sent to SolarWinds engineering managers on January 30, 2018, stating that there was

"improvement needed to be able to meet the security expectation of a Secure Development Lifecycle," and that the SEC argues that what I meant to convey was that the Security Statement's representations about SolarWinds' software development practices were inaccurate. I submit this declaration to explain what I meant in the email and to clarify that I was not intending to contradict the Security Statement's representations about software development, which were true throughout the Relevant Period in this case (October 2018 to January 2021).

3. It is important to understand the context for the email in question. Around this time, SolarWinds, like many companies, was preparing for the European Union (EU)'s General Data Protection Regulation (GPPR) to come into effect in May 2018. The GDPR was a major new data protection regulation that applied to companies doing business in the EU, including SolarWinds and many of SolarWinds' customers. One key expectation of the GDPR is that companies should have documentation available to show they have appropriate data security measures in place. So, in the leadup to the GDPR coming into effect, many companies, including SolarWinds, were examining different aspects of their security programs in order to formalize and improve documentation around them.

4. As part of this effort, I was tasked with reviewing our software development activities to ensure that they were ready for the increased expectations that would come with GDPR. I knew from my years of working as a software engineer at SolarWinds that the Company's engineering teams already conducted security testing—such as vulnerability scans and penetration testing—as part of their software development processes. I had directly participated in numerous software development projects where we conducted such testing. However, I also knew that software engineers are often not diligent at documenting everything they do, and I also knew that development teams varied in terms of how they structured and documented their security activities.

5. So, as part of this project, I created a standardized framework for secure software development that all SolarWinds development teams could use to structure and document their security activities. This included preparing new internal policy documentation describing the secure development processes that all teams should follow, which I referred to as our "Secure Development Lifecycle" or "SDL." As part of the SDL, I created new documentation practices designed to help development teams document their security activities in a consistent way. In particular, I created a requirement that teams prepare a "Final Security Review" prior to any substantial software release, which was intended to be a consolidated record of the security testing and evaluations done during the development process.

6. I also designed an internal training for all software engineers at the Company to familiarize them with the SDL framework I put together and the new documentation requirements it involved. Importantly, this training was designed for *all* software engineers at the Company—even though many of them might not have a security-related role. (For example, an engineer focused on developing the user interface for a piece of software would likely not have any role in doing vulnerability scans or penetration testing of the software.) The purpose of the training was to increase visibility across the Company's engineering organization into our secure development practices and activities and to make sure everyone understood the importance of these activities.

7. It was in this context that I sent out the email cited by the SEC. In late January 2018, I was preparing to start delivering the general SDL training I had developed, which I planned to do in a series of in-person sessions with SolarWinds' various development teams. In anticipation of that, I thought it would be useful for all software development team members to be familiar with what SolarWinds stated publicly about its software development lifecycle in the Company's online Security Statement, which had just recently been added to the Company's website. So, on

January 25, 2018, I sent the "Software Development Lifecycle" section of the Security Statement to all engineering managers, asking them to share it with their teams. *See* Ex. A (SW-SEC00238141) at -141.

8. On January 30, 2018, I received a response from one of the engineering managers, Lukas Vrbecky, who was familiar with my ongoing GDPR-related work to formalize our existing software security processes. Lukas stated in his email, "This is [] great progress in formalizing our security process," and asked if I had any more details to share, including about "upcoming trainings." Ex. B (SW-SEC-SDNY_00055079) at -079. I responded that I was planning to start training soon that would cover the SDL I had developed "at a high level," and that I could "put together an email for managers so they can begin talking with their teams" about it. Ex. B at -079. Lukas wrote back:

> I think that would be great. It came back from teams as a feedback that we actually don't do things and actions that are in the statement. I'd say more accurate would be that teams are not fully aware about the scope of what we do and also what are we going to do by the end of Ql. For these kind of questions coming from team, I'd like managers to have canned answer.

Ex. B at -079.

9. Lukas did not elaborate on what "feedback" he had received from members of the teams under his supervision, but it was not surprising to me that some engineers may not have known about the security testing that was already part of our software development process. In my email message, I had asked engineering managers to share the excerpt from the Security Statement with *all* software engineers, not just those involved in the security aspects of development, so some of the recipients would not have been familiar with those aspects. That is what I understand Lukas to have meant in saying: "I'd say more accurate would be that teams *are not fully aware* about the scope of what we do." *See* Ex. B at -079 (emphasis added).

10. In any event, at the time, my focus was on building interest for the training I was preparing to start in the coming weeks. So, I responded to Lukas's email—which had asked for a "canned answer" that engineering managers could provide in response to any similar feedback—by sending another email to all engineering managers a few hours later, with a response they could provide:

> The simple response is: There is improvement needed to be able to meet the security expectations of a Secure Development Lifecycle. We will be working with teams throughout 2018 to begin incorporating the SDL into their development lifecycle. This begins with general SDL training for all of Engineering along with several SDL pilots with specific teams in Q1. We'll continue to programmatically roll out the SDL to additional teams each quarter.

Ex. A at -141.

11. In stating there was "improvement needed," I wanted to encourage engineers to attend the trainings and to generate interest in the SDL framework that I had developed. Moreover, there *was* improvement that I thought we needed to make to our software development practices. In particular, we needed to improve the documentation we generated around our security testing, especially in light of the heightened regulatory expectations that would come with GDPR. I also wanted to raise awareness of the importance of secure software development among all engineers, which I believed would reinforce our existing security practices. These improvements were the main objective of my trainings.

12. The email I sent was *not* meant to imply that SolarWinds generally did not do the types of security testing referenced in the Security Statement. Again, I knew that we did. The SDL framework that I developed was intended to be an overlay on top of these existing practices, to formalize them and make them more consistent across teams. I was not introducing security practices into the development process where none existed before.

13. I would also note that my email was sent nearly 10 months before SolarWinds' IPO in 2018, which from my understanding is the beginning of the Relevant Period in this case. I know that SolarWinds routinely conducted the sorts of security testing described in the Security Statement during the Relevant Period. Not only do I know this from my own experience as Director of Engineering during the Relevant Period, but I also know it from assisting with document collection for purposes of this litigation. From searching certain internal platforms used by our software development teams to track their work, I found numerous records of vulnerability scans, regression tests, penetration tests, and Final Security Reviews generated as part of the software development process during the Relevant Period, which I understand were subsequently produced to the SEC.

[*signature on following page*]

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: April 23, 2025

Steven Colquitt